Anlage 1

Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO

Stand: Version 1.2 (November 2026)

Diese technischen und organisatorischen Maßnahmen beschreiben das Sicherheitskonzept der DentaTool-Plattform und dienen der Gewährleistung eines dem Risiko angemessenen Schutzniveaus gemäß Art. 32 DSGVO.

Die Maßnahmen werden regelmäßig überprüft und entsprechend dem Stand der Technik fortentwickelt.

1. Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, unbefugten Personen den physischen Zugang zu Systemen und Datenträgern zu verwehren.

Die DentaTool-Plattform wird ausschließlich in professionellen Rechenzentren innerhalb Deutschlands betrieben. Anwendungsserver, Datenbank und Datenbanksicherungen liegen beim Hostinganbieter, hochgeladene Dateien im Objektspeicher von Amazon Web Services in der Region Frankfurt (Anlage 2, Nr. 1 und 6).

Die eingesetzten Hosting- und Speicheranbieter stellen insbesondere folgende Maßnahmen sicher:

- mehrstufige Zutrittskontrollen
- elektronische Zugangssysteme
- Videoüberwachung sicherheitsrelevanter Bereiche
- Einbruchmeldeanlagen
- Alarmierungssysteme
- Brandschutzmaßnahmen
- unterbrechungsfreie Stromversorgung
- Notstromversorgung
- Klimatisierung der Serverräume
- Zugang ausschließlich für autorisierte Personen

Der Auftragnehmer selbst betreibt keine eigenen Serverräume.

2. Zugangskontrolle

Ziel der Zugangskontrolle ist die Verhinderung der Nutzung von IT-Systemen durch unbefugte Personen.

Hierzu werden insbesondere folgende Maßnahmen eingesetzt:

- persönliche Benutzerkonten
- individuelle Benutzerkennungen
- Passwortschutz

sichere Passwortspeicherung mittels moderner Hashverfahren
- verschlüsselte Authentifizierung
- Sitzungsverwaltung
- automatische Sitzungsbeendigung nach Inaktivität
- rollenbasierte Benutzerverwaltung
- Sperrung deaktivierter Benutzerkonten
- verschlüsselte Kommunikation mittels TLS

Soweit verfügbar, unterstützt DentaTool die Verwendung einer Zwei-Faktor-Authentifizierung.

3. Zugriffskontrolle

Ziel der Zugriffskontrolle ist sicherzustellen, dass berechtigte Benutzer ausschließlich auf diejenigen Daten zugreifen können, für die sie autorisiert sind.

Hierzu werden insbesondere eingesetzt:

- Rollen- und Berechtigungskonzept
- Mandantenverwaltung
- Zugriff ausschließlich entsprechend der zugewiesenen Benutzerrolle
- Einschränkung administrativer Rechte
- regelmäßige Überprüfung administrativer Berechtigungen
- Protokollierung administrativer Tätigkeiten
- Least-Privilege-Prinzip
- Dateispeicher ohne öffentlichen Zugriff (Block Public Access); Zugriff nur über die Anwendung mit einem eigenen Dienstkonto, das auf Lesen, Schreiben, Löschen und Auflisten des jeweiligen Speichers beschränkt ist

Administratoren des Auftragnehmers erhalten ausschließlich Zugriff, soweit dies zur Fehleranalyse, Wartung oder Erfüllung vertraglicher Supportleistungen erforderlich ist.

4. Trennungskontrolle

DentaTool ist als mandantenfähige Cloud-Plattform entwickelt.

Die Daten verschiedener Auftraggeber werden logisch voneinander getrennt verarbeitet.

Es ist technisch ausgeschlossen, dass Benutzer eines Auftraggebers auf Daten eines anderen Auftraggebers zugreifen können.

Mandantenbezogene Datenzugriffe werden ausschließlich innerhalb des jeweiligen Mandanten ausgeführt.

Auch interne Verwaltungsfunktionen berücksichtigen die Mandantentrennung.

5. Weitergabekontrolle

Personenbezogene Daten werden ausschließlich auf Weisung des Auftraggebers oder auf gesetzlicher Grundlage an Dritte übermittelt.

Zur Sicherstellung der Vertraulichkeit werden insbesondere eingesetzt:

- TLS-Verschlüsselung bei der Datenübertragung
- verschlüsselte E-Mail-Kommunikation soweit technisch möglich

Zugriff ausschließlich über authentifizierte Benutzerkonten
- Berechtigungskonzepte
- vertragliche Verpflichtung sämtlicher Unterauftragsverarbeiter nach Art. 28 DSGVO

Die KI-Modellverarbeitung erfolgt ausschließlich in den EU-Regionen von Amazon Web Services (Frankfurt, Stockholm, Paris, Mailand, Spanien und Irland). Der Auftragnehmer nutzt dafür ausschließlich EU-Inference-Profile; eine Verarbeitung in Regionen außerhalb der Europäischen Union ist technisch ausgeschlossen. Soweit der Unterauftragsverarbeiter zu einer Unternehmensgruppe mit Sitz außerhalb der Europäischen Union gehört, stellt der Auftragnehmer die Voraussetzungen der Art. 44 ff. DSGVO für etwaige Zugriffe aus Drittländern sicher (siehe Anlage 2). Im Übrigen erfolgt eine Übermittlung personenbezogener Daten in Drittstaaten grundsätzlich nicht.

6. Eingabekontrolle

Zur Nachvollziehbarkeit der Datenverarbeitung werden geeignete Protokollierungsmechanismen eingesetzt.

Soweit technisch vorgesehen, werden insbesondere protokolliert:

- Benutzeranmeldungen
- Änderungen wichtiger Stammdaten
- Erstellung und Änderung von Aufträgen
- Änderungen an Benutzerrechten
- administrative Tätigkeiten
- sicherheitsrelevante Ereignisse

Die Protokollierung dient ausschließlich der Systemsicherheit, Fehleranalyse und Nachvollziehbarkeit.

7. Auftragskontrolle

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich auf dokumentierte Weisung des Auftraggebers.

Mitarbeiter des Auftragnehmers erhalten ausschließlich Zugriff auf personenbezogene Daten, soweit dies

- zur Fehlerbehebung,
- zur Wartung,
- zur Weiterentwicklung der Plattform oder
- zur Erfüllung vertraglicher Supportleistungen

erforderlich ist.

Alle Mitarbeiter sind auf Vertraulichkeit verpflichtet.

Unterauftragsverarbeiter werden ausschließlich nach Abschluss eines Vertrages gemäß Art. 28 DSGVO eingesetzt.

8. Verfügbarkeitskontrolle

Zum Schutz vor Verlust personenbezogener Daten werden unter anderem folgende Maßnahmen eingesetzt:

- regelmäßige Datensicherungen
- redundante Speichersysteme der Hosting- und Speicheranbieter
- Versionierung des Dateispeichers (gelöschte oder überschriebene Dateien sind bis zu 30 Tage wiederherstellbar)
- Monitoring zentraler Systemkomponenten
- automatische Fehlerüberwachung
- Wiederherstellungsverfahren
- Schutz vor Stromausfällen
- Brandschutzmaßnahmen im Rechenzentrum
- redundante Internetanbindungen der Hosting- und Speicheranbieter

Datensicherungen werden regelmäßig überprüft.

9. Verschlüsselung

Zum Schutz personenbezogener Daten werden geeignete Verschlüsselungsverfahren eingesetzt.

Hierzu gehören insbesondere:

- TLS für sämtliche Datenübertragungen
- serverseitige Verschlüsselung der im Objektspeicher abgelegten Dateien (AES-256)
- verschlüsselte Speicherung von Passwörtern mittels moderner Hashverfahren
- verschlüsselte Speicherung sicherheitsrelevanter Zugangsdaten
- verschlüsselte Sicherungskopien, soweit technisch vorgesehen

Kryptographische Verfahren werden regelmäßig entsprechend dem Stand der Technik überprüft.

Schutz besonders sensibler personenbezogener Daten

Zum zusätzlichen Schutz personenbezogener Daten werden ausgewählte Datenfelder mit besonderem Schutzbedarf bereits auf Anwendungsebene verschlüsselt gespeichert.

Hierzu zählen insbesondere personenbezogene Daten, deren Offenlegung ein erhöhtes Risiko für die Rechte und Freiheiten betroffener Personen begründen würde, wie beispielsweise Patientennamen.

Die hierfür eingesetzten kryptographischen Verfahren und Schlüssel werden durch den Auftragnehmer nach dem Stand der Technik verwaltet und regelmäßig überprüft.

Die Verschlüsselung ergänzt die weiteren technischen und organisatorischen Maßnahmen und dient der Verringerung des Risikos eines unbefugten Zugriffs auf personenbezogene Daten.

Die Verschlüsselung erfolgt zusätzlich zu den Maßnahmen der Transportverschlüsselung sowie der Zugriffskontrolle und stellt einen weiteren Baustein des Sicherheitskonzepts der DentaTool-Plattform dar.

10. Wiederherstellbarkeit

Zur Sicherstellung der Wiederherstellbarkeit personenbezogener Daten bestehen Verfahren zur regelmäßigen Datensicherung.

Im Rahmen des Backupkonzeptes werden Datensicherungen erstellt und für einen begrenzten Zeitraum vorgehalten.

Die Wiederherstellung einzelner Systeme kann im Bedarfsfall durchgeführt werden.

11. Belastbarkeit der Systeme

Die Plattform wird kontinuierlich überwacht.

Hierzu gehören insbesondere:

- Servermonitoring
- Fehlerüberwachung
- Ressourcenüberwachung
- Log-Auswertung
- automatische Benachrichtigung bei kritischen Systemzuständen

Sicherheitsupdates werden zeitnah eingespielt.

12. Datenschutz durch Technikgestaltung

Bereits bei Entwicklung neuer Funktionen werden Datenschutzanforderungen berücksichtigt.

Hierzu gehören insbesondere:

- Datenminimierung
- rollenbasierte Berechtigungen
- Mandantentrennung
- sichere Standardkonfigurationen
- datenschutzfreundliche Voreinstellungen
- regelmäßige Sicherheitsüberprüfung neuer Funktionen

Neue Funktionen werden vor ihrer Bereitstellung getestet.

13. Datenschutzfreundliche Voreinstellungen

Standardmäßig werden ausschließlich diejenigen personenbezogenen Daten verarbeitet, die zur Erbringung der jeweiligen Funktion erforderlich sind.

Neue Funktionen werden unter Berücksichtigung des Grundsatzes der Datenminimierung entwickelt.

14. Mitarbeiterschulung

Mitarbeiter des Auftragnehmers werden regelmäßig hinsichtlich

- Datenschutz,
- Informationssicherheit,
- Vertraulichkeit sowie
- sicherem Umgang mit personenbezogenen Daten

sensibilisiert.

Zugriffsberechtigungen werden regelmäßig überprüft und bei Ausscheiden eines Mitarbeiters unverzüglich entzogen.

15. Sichere Softwareentwicklung

Der Auftragnehmer berücksichtigt Anforderungen der Informationssicherheit und des Datenschutzes bereits während der Entwicklung neuer Funktionen der DentaTool-Plattform.

Hierzu gehören insbesondere:

- Entwicklung nach etablierten Grundsätzen sicherer Softwareentwicklung (Secure Development Lifecycle)
- Verwendung einer Versionsverwaltung zur Nachvollziehbarkeit sämtlicher Quellcodeänderungen
- Dokumentation von Änderungen im Rahmen des Entwicklungsprozesses
- Prüfung neuer Funktionen vor deren Bereitstellung in der Produktivumgebung
- Zeitnahe Installation sicherheitsrelevanter Updates für eingesetzte Softwarekomponenten
- Regelmäßige Aktualisierung von Abhängigkeiten und Bibliotheken im Rahmen der technischen Wartung
- Beschränkung des Zugriffs auf Entwicklungs- und Produktivsysteme auf autorisierte Personen
- Verwendung getrennter Entwicklungs-, Test- und Produktivumgebungen, soweit technisch vorgesehen

Neue Funktionen werden vor ihrer Bereitstellung auf ihre technische Funktionsfähigkeit sowie auf erkennbare Sicherheitsrisiken überprüft.

Der Auftragnehmer verfolgt bekannte Sicherheitslücken in den eingesetzten Softwarekomponenten und behebt diese im Rahmen eines risikoorientierten Patchmanagements.

16. Administrativer Zugriff und Support

Der Auftragnehmer beschränkt den Zugriff auf personenbezogene Daten auf diejenigen Mitarbeiter, deren Zugriff zur Erfüllung ihrer jeweiligen Aufgaben erforderlich ist.

Administrativer Zugriff auf Kundendaten erfolgt ausschließlich

- zur Fehleranalyse,
- zur Fehlerbehebung,
- zur Durchführung von Wartungsarbeiten,
- zur Erfüllung vertraglich vereinbarter Supportleistungen oder
- zur Gewährleistung eines sicheren Betriebs der Plattform.

Supportzugriffe erfolgen ausschließlich durch hierzu autorisierte Mitarbeiter.

Der Zugriff wird auf das zur Erfüllung des jeweiligen Zwecks erforderliche Maß beschränkt.

Mitarbeiter des Auftragnehmers sind auf die Vertraulichkeit personenbezogener Daten verpflichtet und werden regelmäßig hinsichtlich Datenschutz und Informationssicherheit sensibilisiert.

Soweit technisch vorgesehen, werden administrative Tätigkeiten protokolliert.

Der Auftragnehmer ist bestrebt, die Möglichkeiten zur Nachvollziehbarkeit administrativer Zugriffe sowie deren technische Einschränkung fortlaufend weiterzuentwickeln.

17. Mandantenfähigkeit und logische Datentrennung

Die DentaTool-Plattform ist als mandantenfähige (Multi-Tenant-)Cloud-Anwendung konzipiert.

Ziel der Mandantenarchitektur ist es, sicherzustellen, dass personenbezogene Daten verschiedener Auftraggeber jederzeit logisch voneinander getrennt verarbeitet werden und ausschließlich berechtigten Benutzern innerhalb des jeweiligen Mandanten zugänglich sind.

Hierzu werden insbesondere folgende Maßnahmen umgesetzt:

- Jeder Auftraggeber erhält einen eigenen logisch getrennten Mandanten innerhalb der Plattform.
- Benutzerkonten sind eindeutig einem Mandanten zugeordnet.
- Datenzugriffe erfolgen ausschließlich innerhalb des jeweils zugeordneten Mandanten.
- Berechtigungen werden serverseitig geprüft und durchgesetzt.
- Benutzer können ausschließlich auf Daten zugreifen, für die ihnen innerhalb ihres Mandanten entsprechende Berechtigungen erteilt wurden.
- Ein Zugriff auf Daten anderer Mandanten ist technisch ausgeschlossen.
- Die Mandantenzuordnung erfolgt zentral innerhalb der Anwendung und wird bei sämtlichen datenverarbeitenden Vorgängen berücksichtigt.
- Administrative Funktionen berücksichtigen die Mandantentrennung und beschränken Zugriffe auf das jeweils erforderliche Maß.

Die Mandantentrennung stellt einen wesentlichen Bestandteil des Sicherheitskonzeptes der DentaTool-Plattform dar und dient dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten personenbezogenen Daten.

18. Regelmäßige Überprüfung und Weiterentwicklung

Der Auftragnehmer überprüft die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen regelmäßig auf ihre Wirksamkeit und Angemessenheit.

Soweit erforderlich, werden die Maßnahmen unter Berücksichtigung des Stands der Technik, technischer Weiterentwicklungen, neuer Bedrohungslagen sowie geänderter gesetzlicher oder regulatorischer Anforderungen angepasst.

Dabei wird sichergestellt, dass das Schutzniveau der Verarbeitung personenbezogener Daten nicht abgesenkt wird.

19. KI-Assistenten (Amazon Bedrock)

Diese Maßnahmen gelten für die KI-Funktionen (Web-Assistent und KI-Auftragszettelerfassung), soweit der Auftraggeber sie nutzt. Abweichend von Ziffer 1 erfolgt die Modellverarbeitung nicht in Rechenzentren in Deutschland, sondern in den EU-Regionen des Unterauftragsverarbeiters Amazon Web Services EMEA SARL (Anlage 2, Nr. 4). Die Plattform selbst wird weiterhin bei dem in Anlage 2 genannten Hostinganbieter betrieben.

Es bestehen insbesondere folgende Maßnahmen:

- Begrenzung auf Mandant und Berechtigte: Der Assistent sieht nur Daten des eigenen Labors; Praxisnutzer sehen nur Daten ihrer eigenen Praxis. Aktionen werden serverseitig gegen die Berechtigungen des handelnden Benutzers geprüft.
- Nutzung nur nach Zustimmung zum AVV: Die KI-Funktionen sind erst nach Zustimmung (Testphase) oder Vertragsschluss verfügbar.

Feste Modellfreigabe: Nur freigegebene Modelle von Amazon Bedrock im EU-Inferenzprofil sind konfigurierbar; eine andere Konfiguration verhindert den Start der Anwendung.

- Keine Aufbewahrung beim Modellanbieter: Aufbewahrung der Ein- und Ausgaben ist in allen Regionen des Profils ausgeschlossen, die Protokollierung der Modellaufrufe ist ausgeschaltet.
- Datenminimierung: Das Modell erhält nur die für die Anfrage nötigen Abfrageergebnisse und den Gesprächsverlauf der jeweiligen Unterhaltung.
- Schutz vor Missbrauch: Mengenbegrenzung der Anfragen je Benutzer und Labor; Inhalte aus Nachrichten werden als Daten behandelt und können die Regeln des Assistenten nicht ändern; bei Fehlern oder Zweifeln erfolgt die Übergabe an das Labor.
- Nachvollziehbarkeit: Ausgeführte Aktionen des Assistenten werden protokolliert; Inhalte von KI-Antworten werden nicht in Betriebsprotokolle geschrieben.
- Löschung: Unterhaltungen werden nach der vom Auftraggeber gewählten Frist (7 Tage, 30 Tage oder 12 Monate seit der letzten Nachricht) automatisch gelöscht.
- Transportverschlüsselung (TLS) zum Modellservice.
- Eigener, beschränkter Zugang zum Modellservice: Der Zugang erfolgt über einen eigens dafür angelegten technischen Zugang, dessen Rechte auf den Modellaufruf in den EU-Regionen beschränkt sind. Er hat keine Rechte für andere Dienste, für die Konfiguration oder für Abonnements.
- Mehrfaktor-Authentifizierung für die Konsole: Die Konsolenzugänge zur Cloud-Umgebung (Administrator und Hauptkonto) sind durch Mehrfaktor-Authentifizierung geschützt.
- Protokollierung von Konfigurationsänderungen: Änderungen und Anmeldungen in der Cloud-Umgebung werden über AWS CloudTrail in allen Regionen protokolliert; die Protokolle liegen in einem nicht öffentlichen Speicher in der EU (Frankfurt), sind durch eine Integritätsprüfung gegen Manipulation geschützt und werden nach 12 Monaten automatisch gelöscht. Die Modellaufrufe selbst und ihre Inhalte werden nicht protokolliert.